REMARKS

In response to the Final Office Action mailed on March 14, 2008, Applicant respectfully requests reconsideration. Claims 1-4, 6-20, 22, 23, 25-32 and 35-37 are pending in this application. Claims 1-4, 6-20, 22, 23, 25-32 and 35-37 are rejected. Claims 1, 10, 20, 29, 31 and 32 are currently amended. Claims 1, 10, 20, 29, 32 and 36 are independent claims, and the remaining claims are dependent claims. Applicant believes that the claims as presented are in condition for allowance. A notice to this affect is respectfully requested.

Claim Amendments

Claims 1, 10, 20 and 32 all have similar amendments to each other. Support for such amendments to claims 1, 10, 20 and 32 is found in the specification on page 16, lines 3-4. Claims 29, 31 and 36 have similar amendments to each other. Support for such amendments to claims 29, 31 and 36 is found in the specification on page 16, lines 3-4, and in figure 2. Thus, no new matter has been added in the claim amendments.

Rejections under 35 U.S.C. §103

Claims 1-4, 6-16, 20, 22-23, 25-32 and 35-37 have been rejected under 35 U.S.C. §103(a) as being unpatentable over Bowe et al. (US 2003/0093678) in view of Cooper et al. (US 2001/0051996). Claims 17-19 and 35 have been rejected under 35 U.S.C. §103(a) as being unpatentable over Bowe et al. (US 2003/0093678) in view of Cooper et al. (US 2001/0051996), and in view of Kato et al. (US 2002/0040431). Applicant traverses this rejection. Applicant respectfully submits that the reference combinations fail to disclose, explicitly or implicitly, the claimed invention as amended.

Claim 1.

Claim 1 includes features not disclosed by Bowe or Cooper. The amendments to claim 1 further clarify how the invention is patentable over the reference combination. Specifically, claim 1 recites:

- "generating, at a server, a signature corresponding to a signature block, the signature block having a covered data portion and an information object portion, the signature computed only on data in the covered data portion, the server conversant in a predetermined protocol and the signature and signature block being conformant with the predetermined protocol;"
- "the signature block further operable to store, in the information object portion, payload data in a nondestructive manner, the nondestructive manner operable to preserve the covered data portion and corresponding signature without regenerating the signature such that the payload data is not included in computing the signature, the covered data portion remaining unwritten by the nonsigning client"

Support for these amendments is found in the Specification on page 16, lines 3-4. This process step may seem counter-intuitive. However, the transmission of the signature block can remain secure via a trusted interface connection between the server and the client, being on the secure side of a network. The secure side may be demarcated by any suitable means, such as firewalls, VPNs (virtual private networks), and SSL (Secure Socket Layer), by way of example only.

In contrast, Bowe teaches at paragraph [0035]:

> "These and other objects are attained by the invention, one aspect of which comprises a signing server that creates a signature for a data object, associates the signature and the data object with a signed object, and later authenticates the signed object. According to the invention, the client computer accesses the signing server,

> such as by using a browser, and then **transmits the data object from the client to the server** via a communications channel such as the Internet. Upon receiving the object, **the server processes the object to generate a signature**, associates the signature with the object to generate a signed object, and transmits the signed object back to the client."

The conventional approach to creating a digital signature is to use a data object as a basis for creating a digital signature. Bowe discloses a server-side digital signature system. Bowe discloses generating a digital signature in a traditional manner, but at a remote server. This is why Bowe discloses transmitting the data object from the client to the server. Bowe then uses the data object to compute a digital signature.

The presently claimed invention teaches away from this approach. The present invention does not transmit the data object/payload data to a remote server to be used in computing a digital signature as in Bowe. Instead, the signature is computed only on data in the covered data portion prior to writing the payload data. The signature block with the computed signature is returned to the remote client, and then payload data, or data object, is appended to the signature block for transmission to a destination.

The previously computed and written signature, therefore, does not encompass the payload data. Such a method is beneficial when operating within a secure network, such as within a virtual private network, or within a physically encapsulated network.

Writing a Check

A good analogy to better understand the differences between the presently claimed invention and Bowe, is that of writing a check for a certain amount. The general process a person follows in writing a check is to indicate a payee, indicate an amount, and then sign the check. The Bowe reference, in this analogy, uses a third-party to sign the check. Following this analogy with the Bowe reference, a person completes the payee portion and the amount portion

on a check. Next, the check is sent to a third-party, such as an accounting department within a company, to be signed. The accounting department actually signs or authorizes the check. The presently claimed invention, however, operates counter intuitively, but is very useful in certain circumstances. Following this analogy with the presently claimed invention, an employee sends a blank check to the accounting department to be signed. The accounting department signs the check and returns the blank, signed check to the employee. The employee then can enter an amount and a payee. Generally, accounting departments would avoid distributing blank checks among employees. If employees in an organization, however, are completely trustworthy, then distributing blank checks can be useful to improve efficiency of a business. Likewise, in the present invention, when the remote client is operating within a trusted network, it is useful to have pre-generated signatures to reduce the computational overhead on the remote client. Especially when the remote client is a cell phone or PDA that does not have the computational resources to efficiently generate digital signatures.

Claim 1, is patentable over the reference combination, because the reference combination fails to teach all the features of the presently claimed invention. Therefore, applicant believes claim 1 to be in condition for allowance.

Claims 10, 20, and 32.

Claims 10, 20, and 32 are all independent claims, and were amended similarly to independent claim 1. Claims 10, 20 and 32 are patentable over the reference combinations under the same rationale as claim 1. Therefore applicant believes claims 10, 20 and 32 are in condition for allowance.

Claims 29, 31, and 36.

Claims 29 and 36 are independent claims, and claim 31 depends on claim 29. Claims 29 and 36 include amendments similar to claim 1, and are patentable over the reference combinations under the same rationale as claim 1. Claims 29,

31 and 36 include further limitations to clarify that payload data is not used to compute the signature, but is appended to the signature block after the remote client receives the signature block. Specifically, Claim 29 recites: "storing the signature value in the signature value portion of the signature block before storing payload data to the information object portion," and claim 31 recites: "storing, after receiving the signature block by the client, the identified payload data in the information object portions." Claim 36 includes both of these amended features.

Claims 2-4, 6-9, 11-19, 22, 23, 25-28, 30, 35 and 37.

Claims 2-4, 6-9, 11-19, 22, 23, 25-28, 30, 35 and 37 all depend on one of independent claims 1, 10, 20, 29, 32, and 36. Because each of the dependent claims incorporates all the limitations of the independent claims from which they depend, Applicant submits that each of the is one claims are allowable by virtue of dependency.

Summary

Applicant respectfully submits that the claims in the subject application are patentable over Bowe, Cooper, and Kato because the reference combinations fails to teach or disclose all of the features of the claimed invention. Thus, Applicant submits that the pending claims are in condition for allowance.

Applicant hereby petitions for any extension of time which is required to maintain the pendency of this case. If there is a fee occasioned by this response, including an extension fee, that is not covered by an enclosed check, please charge any deficiency to Deposit Account No. 50-3735.

/joshuadmather/

Joshua D. Mather, Esq.
Attorney for Applicant(s)
Registration No.: 53,282
Chapin Intellectual Property Law, LLC
Westborough Office Park
1700 West Park Drive
Westborough, Massachusetts 01581
Telephone: (508) 616-9660
Facsimile: (508) 616-9661

Attorney Docket No.: SUN03-06(P9621)

Dated: July 14, 2008